明 細 書

アクセス制御システム、並びにそれに用いられるアクセス制御装置、及びリソース提供装置

技術分野

[0001] 本発明は、電子機器間における一時的なアクセスを制御するアクセス制御システム、並びにそれに用いられるアクセス制御装置、及びアクセス制御システムに用いられ、他の電子機器に対してリソースを提供するリソース提供装置に関する。

背景技術

[0002] 近年、電子機器のマルチユーザ化が進められており、同一の機器を複数のユーザが同時に使用することが可能になっている。例えば、ユーザAが所有する機器にユーザA自身が端末を用いてアクセスすると共に、他のユーザBもまた、ユーザAが所有する機器にアクセスすることができる。

[0003] ネットワークを介してユーザが他者に機器を貸し出す場合、セキュリティが最も重要な要素となる。例えば、物理的に機器を貸し出す場合、ユーザ同士が機器を手渡しし、誰が当該機器を使用するのかを管理することができる。しかしながら、ネットワークを介して、他の電子機器(以下、リソース利用装置と呼ぶ)からリソースを保持する電子機器(以下、リソース提供装置と呼ぶ)へのアクセスを許可し、リソース提供装置の機能を利用できるようにした場合、知らない間に、リソース提供装置が第三者により不正にアクセスされる場合がある。

[0004] 非特許文献1には、この課題を解決するためのプロトコル(以下、「UPnP(Universal Plug and Play)セキュリティ」と呼ぶ)が記載されている。UPnPセキュリティは、リソース利用装置によるリソースの利用を制御する電子機器(以下、アクセス制御装置と呼ぶ)が、ネットワークを介してリソース提供装置を制御するための汎用的なプロトコルである。UPnPセキュリティを使うことで、リソース利用装置からリソース提供装置へのアクセスを制御することができる。

[0005] また、UPnPセキュリティでは、アクセス制御時に発行したアクセス許可の破棄条件を設定することができる。具体的には、発行したアクセス許可に対して有効期間を設

定することができる。これにより、有効期間外におけるアクセスを防止することができる。

[0006] しかしながら、UPnPセキュリティでは、アクセス許可を与える際に有効期間が設定されていない場合、不要となったアクセス許可を速やかに破棄することができない。不要となったアクセス許可は破棄すべきであり、実際に破棄すべき状態となってから実際に破棄されるまでの時間を限りなくゼロに近づける必要がある。

[0007] また、特許文献1には、無線通信機能を備えた複数の電子機器によるアクセスを制御する通信システムが記載されている。特許文献1で定義されている電子機器グループにおいて、電子機器に対してアクセスを許可するアクセス制御装置は、グループ内の1つの電子機器の存在が確認できなくなると、グループ内の全ての電子機器からのアクセスを禁止する。

特許文献1:特開2003－289307号公報

非特許文献1:「ユーピーエヌピー デバイス セキュリティ アンド セキュリティ コンソール ブイ(UPnP Device Security and Security Console V)」、[online]、2003年、ユーピーエヌピー フォーラム(UPnP Forum)、インターネット<URL: HYPERLINK "http://www.upnp.org/standardizeddcps/security.asp" http://www.upnp.org/standardizeddcps/security.asp>

発明の開示

発明が解決しようとする課題

[0008] しかしながら、特許文献1に記載の従来の通信システムでは、存在が確認できない電子機器があると、電子機器グループに所属する全ての機器の使用を停止させてしまうものであり、電子機器グループに所属する電子機器であって存在が確認できる電子機器からのアクセスまでも制限してしまう場合が生じてしまい、アクセスを破棄すべき電子機器のみを破棄すべきものではなかった。

[0009] それゆえに、本発明の目的は、上記従来の課題を解決するものであり、破棄すべきアクセス許可を速やかに破棄し、リソースを提供する機器の不正な使用を防止することができるアクセス制御システム、並びにそれに用いられるアクセス制御装置、及びリソース提供装置を提供することである。

課題を解決するための手段

[0010] 本発明は、リソース提供装置で提供されるリソースを利用するために行われるリソース利用装置からリソース提供装置へのアクセスを制御するアクセス制御装置であって、リソース利用装置及びリソース提供装置と通信する通信部と、リソース利用装置からのアクセスを許可するよう、通信部を介してリソース提供装置へ命令するアクセス許可部と、アクセス許可部によってアクセスが許可されたリソース利用装置に関する情報を管理情報として格納する記憶部と、記憶部に管理情報が格納されているリソース利用装置との通信状態を通信部を介して確認する存在確認部と、存在確認部によって通信が途絶えたと判断されたリソース利用装置からのアクセスを拒否するよう、通信部を介してリソース提供装置へ命令するアクセス破棄部とを備える。

[0011] 本発明によれば、アクセス制御装置は、リソース利用装置との通信が途絶えると、当該リソース利用装置からのアクセスを拒否するようリソース提供装置に命令する。これにより、アクセスを破棄すべきリソース利用装置から提供装置への不正なアクセスを防止することができる。

[0012] 好ましくは、アクセス破棄部は、通信が途絶えたと判断されたリソース利用装置に関する情報を記憶部から削除するとよい。これにより、不要な情報がアクセス制御装置内部に残らない。

[0013] 例えば、リソース利用装置に関する情報は、リソース利用装置を識別するための情報であってもよく、また、リソース利用装置を識別するための情報と、当該リソース利用装置からのアクセスを受け付けるリソース提供装置を識別するための情報とを含むものであってもよい。リソース利用装置に関する情報が、リソース提供装置を識別するための情報を含む場合、リソース利用装置がアクセスするリソース提供装置を速やかに特定することができる。

[0014] また、リソース利用装置に関する情報は、リソース利用装置がリソース提供装置へアクセスする際に発行するコマンドに関する情報を含んでいてもよい。これにより、リソース利用装置が利用することができるリソースが複数種類ある場合においても、コマンドの種類を細かく管理することができる。

[0015] また、アクセス許可部は、アクセスを許可すべきリソース利用装置に関する情報を、

通信部を介してリソース提供装置へ通知してもよい。これにより、リソース提供装置は、アクセスを許可すべきリソース利用装置を速やかに特定することができる。

[0016] また、アクセス破棄部は、通信が途絶えたと判断されたリソース利用装置に関する情報を、通信部を介してリソース提供装置へ通知してもよい。これにより、リソース提供装置は、アクセスを拒否すべきリソース利用装置を速やかに特定することができる。

[0017] さらに、通信部を介してリソース提供装置から通信状態の確認要求を受け取ると、当該通信部を介して当該リソース提供装置へ応答する生存確認応答部を備えていてもよい。これにより、アクセス制御装置とリソース提供装置との間の通信状態をリソース提供装置に把握させることができる。

[0018] 通信部は、リソース利用装置と無線を介して通信し、無線による通信範囲は所定の範囲に制限されていてもよい。これにより、アクセス制御装置及びリソース利用装置が所定の範囲内にある場合にのみ、リソース利用装置がリソース提供装置のリソースを利用可能にすることができる。したがって、システムの秘匿性をさらに向上させることができる。

[0019] また、本発明は、アクセス制御装置よりアクセスが許可されたリソース利用装置からのアクセスを受け付け、リソースを提供するリソース提供装置であって、アクセス制御装置及びリソース利用装置と通信する通信部と、通信部を介してアクセス制御装置から命令されたリソース利用装置に関する情報を管理情報として格納する記憶部と、記憶部に管理情報が格納されているリソース利用装置からのアクセスを許可するアクセス許可部と、アクセス制御装置との通信状態を通信部を介して確認する存在確認部と、存在確認部によって通信が途絶えたと判断されたアクセス制御装置によってアクセスが許可されたリソース利用装置からのアクセスを拒否するアクセス拒否部とを備える。

[0020] これにより、リソース提供装置は、アクセス制御装置との通信が途絶えると、当該アクセス制御装置によってアクセスが許可されたリソース利用装置からのアクセスを拒否する。これにより、アクセスを破棄すべき可能性のあるリソース利用装置からリソース提供装置へのアクセスを排除することができる。

[0021] 好ましくは、アクセス拒否部は、通信が途絶えたと判断されたアクセス制御装置によってアクセスが許可されたリソース利用装置に関する情報を記憶部から削除するとよい。これにより、不要な情報がリソース提供装置内部に残らない。

[0022] 例えば、リソース利用装置に関する情報は、リソース利用装置を識別するための情報であってもよく、また、リソース利用装置を識別するための情報と、当該リソース利用装置に対してアクセスを許可したアクセス制御装置を識別するための情報とを含むものであってもよい。リソース利用装置に関する情報が、アクセス制御装置を識別するための情報を含む場合、リソース利用装置にアクセスを許可したアクセス制御装置を速やかに特定することができる。

[0023] また、リソース利用装置に関する情報は、リソース利用装置がリソース提供装置へアクセスする際に発行するコマンドに関する情報を含んでいてもよい。

[0024] また、アクセス拒否部は、リソース利用装置からのアクセスを拒否するよう、通信部を介してアクセス制御部から命令されると、命令されたリソース利用装置からのアクセスを拒否することとしてもよい。これにより、アクセス制御装置がアクセスを許可しないリソース利用装置に対するアクセス拒否を速やかに開始することができる。

[0025] 好ましくは、アクセス拒否部は、命令されたリソース利用装置に関する情報を記憶部から削除するとよい。

[0026] また、通信部は、アクセス制御装置と無線を介して通信し、無線による通信範囲は所定の範囲に制限されていてもよい。

[0027] また、本発明は、リソースを提供するリソース提供装置と、当該リソースへアクセスするリソース利用装置と、当該リソース利用装置によるアクセスを制御するアクセス制御装置とを備えるアクセス制御システムであって、アクセス制御装置は、リソース利用装置及びリソース提供装置と通信する通信部と、リソース利用装置からのアクセスを許可するよう、通信部を介してリソース提供装置へ命令するアクセス許可部と、アクセス許可部によってアクセスが許可されたリソース利用装置に関する情報を管理情報として格納する記憶部と、記憶部に管理情報が格納されているリソース利用装置との通信状態を通信部を介して確認する存在確認部と、存在確認部によって通信が途絶えたと判断されたリソース利用装置からのアクセスを拒否するよう、通信部を介してリソ

ース提供装置へ命令するアクセス破棄部とを含み、リソース提供装置は、アクセス制御装置及びリソース利用装置と通信するリソース提供通信部と、リソース提供通信部を介してアクセス制御装置から命令されたリソース利用装置に関する情報を管理情報として格納するリソース提供記憶部と、リソース提供記憶部に管理情報が格納されているリソース利用装置からのアクセスを許可するリソースアクセス許可部と、アクセス制御装置との通信状態をリソース提供通信部を介して確認するリソース提供存在確認部と、リソース提供存在確認部によって通信が途絶えたと判断されたアクセス制御装置によってアクセスが許可されたリソース利用装置、及びリソース提供通信部を介してアクセス制御装置から命令されたリソース利用装置からのアクセスを拒否するアクセス拒否部とを含む。

発明の効果

[0028] 本発明によれば、破棄すべきアクセス制御を速やかに破棄し、リソースを提供する機器の不正な使用を防止することができるアクセス制御システム、並びにそれに用いられるアクセス制御装置、及びリソース提供装置が提供される。

図面の簡単な説明

[0029] [図1]図1は、本発明の一実施形態に係るアクセス制御システムの全体的な構成の一例を示す図である。

[図2]図2は、アクセス制御処理に用いられる許可情報管理テーブル104の構成の一例を示す図である。

[図3]図3は、リソースアクセス制御処理に用いられるアクセス管理テーブル204の構成の一例を示す図である。

[図4]図4は、アクセス制御装置10の構成を示すブロック図である。

[図5]図5は、アクセス許可命令、アクセス許可通知命令、完了通知、及びアクセス許可破棄命令のデータ構造の一例を示す図である。

[図6]図6は、リソース提供装置20の構成を示すブロック図である。

[図7]図7は、リソース利用装置30の構成を示すブロック図である。

[図8]図8は、アクセス制御装置10によるアクセス制御の流れの一例を示すシーケンス図である。

[図9]図9は、リソース提供装置20によるリソースアクセス制御の流れの一例を示すシーケンス図である。

[図10]図10は、アクセス制御装置10におけるアクセス許可部106、存在確認部107及びアクセス破棄部108の動作を示すフローチャートである。

[図11]図11は、アクセス制御装置10における存在確認応答部105の動作を示すフローチャートである。

[図12]図12は、リソース提供装置20の動作を示すフローチャートである。

[図13]図13は、リソース提供装置20におけるアクセス破棄部207の動作を示すフローチャートである。

[図14]図14は、リソース利用装置30の動作を示すフローチャート

発明を実施するための最良の形態

[0030] 以下、本発明の実施の形態について、図面を参照しながら説明する。

[0031] 図1は、本発明の一実施形態に係るアクセス制御システムの全体的な構成の一例を示す図である。図1において、アクセス制御システムは、アクセス制御装置10と、リソース提供装置20と、リソース利用装置30とを備える。アクセス制御装置10、リソース提供装置20及びリソース利用装置30は、通信機能を有し、それぞれ独立して存在する電子機器である。以下、アクセス制御装置10、リソース提供装置20及びリソース利用装置30を特に区別する必要がない場合には、これらを電子機器と総称する。

[0032] アクセス制御装置10及びリソース提供装置20は接続40を介して、リソース提供装置及びリソース利用装置30は接続50を介して、リソース利用装置30及びアクセス制御装置10は接続60を介して、相互に通信可能に接続される。接続40～60は通信路であり、電子機器をそれぞれ接続する。接続40～60は、例えば、インターネットなどのネットワークを介した接続や、無線を用いた接続、ネットワークケーブル等の有線通信路を用いた接続である。

[0033] なお、図1では、アクセス制御装置10、リソース提供装置20及びリソース利用装置30がそれぞれ1台ずつ存在する場合を示しているが、アクセス制御装置10、リソース提供装置20及びリソース利用装置30は、それぞれ2台以上存在していてもかまわない。

[0034] アクセス制御装置10は、リソース提供装置20と通信し、リソース提供装置20が保持するリソースへのリソース利用装置30からのアクセスを制御する。以下、アクセス制御装置10によるリソース利用装置30のアクセスを制御する処理をアクセス制御処理という。アクセス制御装置10は、一定時間毎にリソース利用装置30と信号を送受信し、リソース利用装置30の存在を確認する。ここで、「存在を確認する」とは、通信相手先(ここでは、リソース利用装置30)と通信可能であることを確認することをいう。アクセス制御装置10は、リソース利用装置30の存在が確認できなかった場合、つまり、リソース利用装置30との通信が途絶えた場合、存在が確認できなかったリソース利用装置30からアクセスを拒否するようリソース提供装置20に命令する。

[0035] リソース提供装置20は、アクセス制御装置10の命令に従い、リソース利用装置30からのアクセスを許可または拒否する。また、リソース提供装置20は、アクセス制御装置10と通信し、リソース利用装置30からのアクセスを制御する。以下、リソース提供装置20によるリソース利用装置30のアクセスを制御する処理をリソースアクセス制御処理という。具体的には、リソース提供装置20は、一定時間毎にアクセス制御装置10の存在を確認する。アクセス制御装置10の存在が確認できなくなった場合、アクセス制御装置10がアクセスを許可したリソース利用装置30からのアクセスを拒否する。

[0036] リソース利用装置30は、リソース提供装置20に一時的にアクセスし、リソース提供装置20のリソースを利用する。ここで、「リソースの利用」とは、アクセス利用装置30がアクセス提供装置20にアクセスし、アクセス提供装置20が有する機能の一部または全部を利用することをいう。例えば、リソース利用装置30は、リソース提供装置20保持する記憶データにアクセスしたり、リソース提供装置20が構成されるデバイスへデータを入出力したりする。

[0037] このように、本実施形態に係るアクセス制御システムの大きな特徴は、アクセス制御装置10がリソース利用装置30を監視し、リソース提供装置20がアクセス制御装置10を監視することにより、第三者がリソース利用装置30を利用してリソース提供装置20へ不正にアクセスすることを防止することである。

[0038] 図2は、アクセス制御処理に用いられる許可情報管理テーブル104の構成の一例を示す図である。アクセス制御装置10は、自装置が保持する許可情報管理テーブ

ル104に基づき、リソース利用装置30のアクセスを制御する。

[0039] 許可情報管理テーブル104には、アクセス制御装置10がアクセスを許可したリソース利用装置30に関する情報が管理情報として記録されている。管理情報は、リソース提供装置20の装置ID(提供側11)と、リソース利用装置30の装置ID(利用側12)と、通信インターフェース(通信I／F13)に関する情報と、アクセス内容に関する情報(アクセス14)とを含む。

[0040] 提供側11には、リソース提供装置20を識別するための装置IDが記録される。装置IDは、リソース提供装置20を一意に特定することができる情報であればよく、例えば、リソース提供装置20のIPアドレスやMACアドレス、リソース提供装置20の公開鍵、リソース提供装置20の公開鍵のハッシュ値等である。以下、装置IDが、IPアドレスである場合を例に説明する。

[0041] 利用側12には、リソース利用装置30を識別するための装置IDが記録される。装置IDは、リソース利用装置30を一意に特定することができる情報であればよく、例えば、リソース利用装置30のIPアドレスやMACアドレス、リソース利用装置30の公開鍵、リソース利用装置30の公開鍵のハッシュ値等である。

[0042] 通信I／F13は、アクセス制御装置10がリソース利用装置30の存在を確認する際に利用する通信インターフェースに関する情報が記録される。例えば、「eth0」は、イーサネット(登録商標)を利用した有線ケーブルを用いた通信であることを示し、「eth1」は、Bluetooth(登録商標)などの無線を利用した通信であることを示す。「ttySO」は、シリアル接続した通信であることを示し、「ANY」は、アクセス制御装置10が装備する通信インターフェースを利用した通信であることを示す。また、例えば、IPネットワークを介して通信する際に、2点の通信における距離をHOPという論理単位で計算することができる場合、通信I／F13は、1HOP以内などと制限してもよい。

[0043] アクセス14には、リソース提供装置20が保持するリソースのうち、リソース利用装置30がアクセスする内容に関する情報が記録される。具体的には、アクセス14には、リソース利用装置30が利用することができるコマンドと、当該コマンドに対するパラメータ(以下、パラメータ制限と呼ぶ)に関する情報が記録される。図6に示す例では、より理解しやすくするために、コマンド及びパラメータ制限に関する情報の組み合わせに

より実現される機能を示している。

[0044] 例えば、リソース利用装置30に許可されたアクセスが「秘密資料参照」である場合、アクセス14には、ファイルを読み出して表示するためのコマンド、及び特定のユーザに対してのみ、その配下にあるファイルを参照できるディレクトリの情報がパラメータ制限に関する情報として記録されている。また、リソース利用装置30に許可されたアクセスが「ビデオ視聴」である場合、アクセス14には、映像関連のファイルを読み出して表示するためのコマンド、及び当該映像関連のファイルを格納するディレクトリの情報がパラメータ制限に関する情報として記録されている。リソース利用装置30に許可されたアクセスが「印刷」である場合、アクセス14には、リソース利用装置30がリソース提供装置20に印刷処理を依頼する際に必要なコマンドが記録されている。リソース利用装置30に許可されたアクセスが「リモコン制御」である場合、アクセス14には、リソース利用装置30がリソース提供装置20を遠隔操作する際に必要なコマンドが記録されている。リソース利用装置30に許可されたアクセスが「ファイル書き込み」である場合、アクセス14には、リソース利用装置30がリソース提供装置20の管理するファイルへデータを書き込む際に必要なコマンドが記録されている。

[0045] アクセス制御装置10は、上記の許可情報管理テーブル104に基づき、以下のようにアクセス制御処理を行う。まず、アクセス制御装置10は、リソース利用装置30へアクセス許可を与えるとき、許可情報管理テーブル104に一行を追加する。また、アクセス制御装置10は、利用側12の各行に記録されているリソース利用装置30の存在を一定時間毎に確認する。リソース利用装置30の存在が確認できなかった場合、アクセス制御装置10は、存在が確認できなかったリソース利用装置30からのアクセスを拒否するようアクセス提供装置20へ命令すると共に、すなわち、存在が確認できなかったリソース利用装置30に関する情報、すなわち、許可情報管理テーブル104の対象の行を削除する。

[0046] 図3は、リソースアクセス制御処理に用いられるアクセス管理テーブル204の構成の一例を示す図である。リソース提供装置20は、自装置が保持するアクセス管理テーブル204に基づき、リソース利用装置30からのアクセスを制御する。

[0047] アクセス管理テーブル204には、リソース利用装置30を識別するための装置ID(利

用側22)、及び利用側22が利用するリソースの内容(アクセス23)が、アクセス制御装置10を識別するための装置ID(制御側21)に対応付けて記録される。

[0048] 制御側21には、アクセス許可命令を発行したアクセス制御装置10を識別するための装置IDが記録される。アクセス許可命令は、リソース提供装置20に対して、リソース利用装置30からのアクセス許可を与えるための命令である。制御側21に記録される装置IDは、アクセス制御装置10を一意に特定することができる情報であればよく、例えば、アクセス制御装置10のIPアドレスやMACアドレス、アクセス制御装置10の公開鍵、アクセス制御装置10の公開鍵のハッシュ値等である。

[0049] 利用側22は、制御側21によって制御されるリソース利用装置30を識別するための装置IDが記録される。装置IDは、リソース利用装置30を一意に特定することができる情報であればよく、例えば、リソース利用装置30のIPアドレスやMACアドレス、リソース利用装置30の公開鍵、リソース利用装置30の公開鍵のハッシュ値等である。

[0050] アクセス23は、リソース提供装置20が保持するリソースのうち、リソース利用装置30がアクセスする内容に関する情報が記録される。具体的には、アクセス14には、リソース利用装置30が利用することができるコマンドと、当該コマンドに対するパラメータ制限に関する情報が記録される。リソース提供装置20は、リソース利用装置30からアクセス命令を受け取ると、アクセス管理テーブル204を参照して利用側22に対応するアクセス23に基づき、リソース利用装置30にアクセスを許可すべきか否かを判断する。

[0051] 次に、アクセス制御装置10、リソース提供装置20及びリソース利用装置30の構成の詳細について説明する。

[0052] 図4は、アクセス制御装置10の構成を示すブロック図である。アクセス制御装置10は、記憶部103と、アクセス制御部102と、通信部101とを含む。記憶部103は、許可情報管理テーブル104を格納する。

[0053] アクセス制御部102は、アクセス許可部106と、アクセス破棄部108と、存在確認部107とを有する。

[0054] アクセス許可部106は、リソース提供装置20へアクセスするリソース利用装置30に関する情報を、アクセス制御装置10が備える入力部(図示せず)から受け取って許可

情報管理テーブル104に記録する。リソース利用装置30に関する情報は、アクセス制御装置10が備える入力部を介してユーザによって入力されてもよく、また、アクセス利用装置30から送信してもよい。また、リソース利用装置30に関する情報をあらかじめアクセス制御装置10の記憶部103に格納しておき、その中から選択し、入力することとしてもよい。

[0055] アクセス許可部106は、許可情報管理テーブル104に記録したリソース利用装置30からのアクセスを許可するようリソース提供装置20へ命令する。具体的には、アクセス許可部106は、アクセス許可命令を生成して通信部101に渡す。

[0056] 図5は、アクセス許可命令のデータ構造の一例を示す図である。図5において、アクセス許可命令は、タイプと、装置IDと、1つ以上の制御情報とを含む。

[0057] タイプは、命令がアクセス許可命令であることを特定するための情報であり、例えば定数である。装置IDは、リソース利用装置30を識別するための情報である。装置IDは、リソース利用装置30を一意に特定することができる情報であればよく、例えば、リソース利用装置30のIPアドレスやMACアドレス、リソース利用装置30の公開鍵、リソース利用装置30の公開鍵のハッシュ値等である。

[0058] 制御情報は、アクセス制御に用いられるコマンドの名前と、コマンドに対するゼロ以上のパラメータ制限と呼ぶとからなる。パラメータ制限は、コマンドの引数、及び影響を及ぼす範囲(例えばディレクトリなど)を示す情報である。

[0059] 図4の説明に戻り、アクセス許可部106は、リソース提供装置20から、リソース利用装置30からのアクセスを受け付け可能となったことを通知する信号(以下、完了通知と呼ぶ)を通信部101を介して受け取ると、リソース提供装置20へのアクセスを許可することをリソース利用装置30へ通知する。具体的には、アクセス許可部106は、アクセス許可通知命令を生成して通信部101に渡す。アクセス許可通知命令のデータ構造は、図5に示すアクセス許可命令のデータ構造と同様であるため、図5を援用する。図5に示すタイプにはアクセス許可通知命令であることを示す定数、装置IDにはリソース利用装置30の装置ID、制御情報のコマンド名にはリソース利用装置30側から発行できるコマンドの名前、パラメータ制限にはコマンドの引数、及び影響を及ぼす範囲(例えばディレクトリなど)を示す情報がそれぞれ記録される。

[0060] 存在確認部107は、許可情報管理テーブル104に記録されているリソース利用装置30がネットワーク上に存在しているか否かを判断する。具体的には、存在確認部107は、存在確認命令を生成して通信部101に渡し、リソース利用装置30から送信されてくる応答を通信部101を介して受け取ることにより、リソース利用装置30の存在を確認する。また、存在確認部206は、リソース利用装置30の存在が確認できない場合、つまり、リソース利用装置30からの応答を受け取ることができなかった場合、当該リソース利用装置30の装置IDをアクセス破棄部207に通知する。

[0061] ここで、通信相手先の存在を確認する方法は、特に限定がないが、例えば、ピング(Ping;Packet INternet Groper)などのTCP／IPネットワークを診断するためのプログラムを利用する方法がある。この方法を用いれば、通信相手先のIPアドレスを指定すると、ICMP(Internet Control Message Protocol)を用いてデータを送信し、通信相手先から応答があるか否かを確認することができる。

[0062] アクセス破棄部108は、存在確認部107から装置IDが通知されると、通知された装置IDを有するリソース利用装置30に発行したアクセス許可を破棄し、当該リソース利用装置30からのアクセスを拒否するようリソース提供装置20へ命令する。具体的には、アクセス破棄部108は、アクセス許可破棄命令を生成し、通信部101に渡す。アクセス許可破棄命令のデータ構造は、図5に示すアクセス許可命令のデータ構造と同様であるため、図5を援用する。図5に示すタイプにはアクセス許可破棄命令であることを示す定数、装置IDにはリソース利用装置30の装置ID、制御情報のコマンド名にはリソース利用装置30側から発行できるコマンドの名前、パラメータ制限にはコマンドの引数、及び影響を及ぼす範囲(例えばディレクトリなど)を示す情報がそれぞれ記録される。

[0063] 図4の説明に戻り、アクセス破棄部108は、許可情報管理テーブル104を参照し、アクセス許可破棄命令に記録した装置IDを有するリソース利用装置30に関する情報を削除する。

[0064] 存在確認応答部105は、他の電子機器(ここでは、リソース提供装置20)からの存在確認命令を通信部101を介して受け取ると、応答を生成して通信部101に渡す。

[0065] 通信部101は、ネットワークとのインターフェースであって、ネットワークから受信した

命令を存在確認部107に渡す。また、通信部101は、アクセス許可部106、アクセス破棄部108、及び存在確認部107から送信すべき命令を受け取ると、当該命令をネットワークへ送信する。

[0066] 図6は、リソース提供装置20の構成を示すブロック図である。リソース提供装置20は、記憶部203と、リソースアクセス制御部202と、通信部201と、リソースアクセス許可部205とを含む。記憶部203は、アクセス管理テーブル204を格納する。

[0067] リソースアクセス許可部205は、アクセス制御装置10から送信されてきたアクセス許可命令を通信部201を介して受け取ると、アクセス許可命令に記録されている情報を読み出し、アクセス管理テーブル204に記録する。例えば、アクセス許可命令に記録されている装置IDがIPアドレスである場合、リソースアクセス許可部205は、アクセス制御装置10のIPアドレスに対応付けて、アクセス許可命令に記録されている装置ID、コマンド及びパラメータ制限に関する情報をアクセス管理テーブル204に記録する。アクセス許可命令に記録されている装置IDがIPアドレス以外の情報である場合、当該装置IDに対応するIPアドレスを検索し、当該IPアドレスに対応付けて、アクセス許可命令に記録されているコマンド及びパラメータ制限に関する情報をアクセス23としてアクセス管理テーブル204に記録してもよい。これと共に、リソースアクセス許可部205は、リソース利用装置30と通信するための設定を行い、設定が完了すると、アクセス制御装置10へ送信するための完了通知を生成して通信部201に渡す。

[0068] 完了通知のデータ構造は、図5に示すアクセス許可命令のデータ構造と同様であるため、図5を援用する。図5に示すタイプには完了通知であることを示す定数、装置IDにはリソース利用装置30のIPアドレス、制御情報のコマンド名にはリソース利用装置30側から発行できるコマンドの名前、パラメータ制限にはコマンドの引数、及び影響を及ぼす範囲(例えばディレクトリなど)を示す情報がそれぞれ記録される。

[0069] 図6の説明に戻り、リソースアクセス許可部205は、リソース利用装置30から、リソース提供装置20が保持するリソースへアクセスするためのアクセス命令を受け取ると、当該リソース利用装置30からのアクセスを許可すべきか否かを判断する。具体的には、リソースアクセス許可部205は、リソース利用装置30から送信されてきたアクセス命令を通信部201を介して受け取ると、アクセス管理テーブル204を参照し、アクセ

ス命令の送信元のリソース利用装置30に関する情報が記録されているか否かを判断する。リソースアクセス許可部205は、送信元のリソース利用装置30に関する情報がアクセス管理テーブル204に記録されている場合、アクセスを許可し、送信元のリソース利用装置30に関する情報がアクセス管理テーブル204に記録されていない場合、アクセスを拒否する。

[0070] リソースアクセス制御部202は、アクセス破棄部207と、存在確認部206とを有し、リソース提供装置20が保持するリソースへのリソース利用装置30によるアクセスを制御する。

[0071] 存在確認部206は、アクセス管理テーブル204に記録されているアクセス制御装置10がネットワーク上に存在しているか否かを判断する。具体的には、存在確認部206は、存在確認命令を生成して通信部201に渡し、アクセス制御装置10から送信されてくる応答を通信部201を介して受け取ることにより、アクセス制御装置10の存在を確認する。また、存在確認部206は、アクセス制御装置10の存在が確認できない場合、つまり、アクセス制御装置10からの応答を受け取ることができなかった場合、当該アクセス制御装置10の装置IDをアクセス破棄部207に通知する。

[0072] アクセス破棄部207は、存在確認部206から装置IDが通知されると、アクセス管理テーブル204を参照し、通知された装置IDを有するアクセス制御装置10に関する情報を削除する。また、アクセス破棄部207は、リソース利用装置30からのアクセスの拒否を命令されると、当該リソース利用装置30からのアクセスを拒否する。具体的には、アクセス破棄部207は、アクセス制御装置10から送信されてくるアクセス許可破棄命令を通信部201を介して受け取ると、アクセス管理テーブル204を参照し、アクセス許可破棄命令に記録されている装置IDを有するリソース利用装置30に関する情報を削除する。

[0073] 通信部201は、ネットワークとのインターフェースであって、ネットワークから受信したメッセージを存在確認部206、アクセス破棄部207、またはリソースアクセス許可部205に渡す。通信部201は、存在確認命令に対する応答を受信すると、当該応答を存在確認部206に渡し、アクセス許可破棄命令を受信すると、当該アクセス許可破棄命令をアクセス破棄部207に渡す。また、通信部201は、アクセス命令を受信すると

、当該アクセス命令をリソースアクセス許可部205に渡す。また、通信部101は、アクセス破棄部207または存在確認部206から送信すべき命令を受け取ると、当該命令をネットワークへ送信する。

[0074] 図7は、リソース利用装置30の構成を示すブロック図である。リソース利用装置30は、通信部301と、存在確認応答部302と、アクセス命令部303とを含む。

[0075] 通信部301は、ネットワークとのインターフェースであって、ネットワークから受信したメッセージを存在確認応答部302、またはアクセス命令部303に渡す。通信部301は、存在確認命令を受信すると、当該存在確認命令を存在確認応答部302に渡す。また、通信部101は、存在確認応答部302またはアクセス命令部303から送信すべき命令を受け取ると、当該命令をネットワークへ送信する。

[0076] 存在確認応答部302は、他の電子機器(ここでは、アクセス制御装置10)からの存在確認命令を通信部301を介して受け取ると、これに応答するための応答信号を生成して通信部301に渡す。

[0077] アクセス命令部303は、アクセス制御装置10から送信されてくるアクセス許可通知命令を通信部301を介して受け取った後、リソース提供装置20に対して所望の処理を行うためのアクセス命令を生成して通信部301に渡す。これにより、リソース利用装置30は、リソース提供装置の機能を利用することが可能となる。アクセス命令は、リソース利用装置30の装置IDと制御情報とを含む。制御情報は、コマンド名と、コマンドの引数及び影響を及ぼす範囲(例えばディレクトリなど)を示すパラメータ制限に関する情報とが記録される。なお、装置IDとしてIPアドレスを用いる場合、装置IDはアクセス命令に記録されなくてもよい。

[0078] 図8は、アクセス制御装置10によるアクセス制御の流れの一例を示すシーケンス図である。

[0079] リソース利用装置30によるリソースの利用を制御するために、アクセス制御装置10とアクセス提供装置20とは、事前準備を行う。例えば、アクセス制御装置10及びリソース提供装置20は、通信路(ここでは、接続40)を介して相互に通信可能な状態を確立する。その方法は公知のものであり、例えば、非特許文献1に記載されているUPnPの技術を利用して、それぞれがネットワークに接続されたことを自動的に認識し

、IPアドレス等の接続に必要な情報を互いに取得した後、相互に通信可能な状態を確立してもよい。また、ユーザが、それぞれの機器が備える入力部(図示せず)から接続に必要な情報を直接入力してもよい。図2では、事前準備がすでに行われており、リソース提供装置20がアクセス制御装置10からの命令を認証していて許可があると認めているものとして説明する。

[0080] まず、アクセス制御装置10は、リソース提供装置20を一時的に利用するリソース利用装置30に関する情報を許可情報管理テーブル104に記録する。この場合も、アクセス制御装置10とリソース提供装置20との間の接続を確立する場合と同様に、UPnPの技術を利用して、アクセス制御装置10とリソース利用装置30との接続に必要な情報を取得してもよく、また、ユーザが入力部から接続に必要な情報を直接入力してもよい。

[0081] そして、アクセス制御装置10は、アクセス許可命令を生成してリソース提供装置20へ送信する(ステップS101)。リソース提供装置20は、受信したアクセス許可命令に記録されている情報のうち、必要な情報をアクセス管理テーブル204に記録すると共に、リソース利用装置30と通信するための設定を行い、設定が完了すると、完了通知を生成してアクセス制御装置10へ送信する(ステップS102)。

[0082] アクセス制御装置10は、完了通知を受信すると、アクセス許可通知命令を生成し、リソース利用装置30へ送信する(ステップS103)。

[0083] 次に、アクセス制御装置10は、アクセス許可命令の送信後、一定時間毎にリソース利用装置30の存在を確認する(ステップS104)。リソース利用装置30の存在が確認できた場合(ステップS105)、アクセス制御装置10はアクセス許可破棄命令を生成しない。

[0084] ステップS101及びステップS102が行われた後、リソース利用装置30は、アクセス制御が必要なリソースを保持するアクセス提供装置20へアクセスするためのアクセス命令を生成してリソース提供装置20へ送信する(ステップS106)。リソース提供装置20は、アクセス命令を受信すると、アクセス管理テーブル204を参照し、アクセス命令を許可すべきか否かを判断する。具体的には、リソース提供装置20は、受信したアクセス命令に記録されているコマンド及び装置IDが、アクセス管理テーブル204に

記録されているコマンド及び装置IDと一致するか否かを判断する。リソース提供装置20は、コマンド及び装置IDが一致した場合にのみアクセスを許可する。これにより、コマンドに応じた処理が実行され、リソース利用装置30によるリソースの利用が可能となる。

[0085] アクセス制御装置10は、一定時間毎にリソース利用装置30の存在を確認し続け、リソース利用装置30の存在が確認できない場合(ステップS107)、アクセス制御装置10は、リソース提供装置20へのアクセス許可命令を破棄すべきであると判断する。

[0086] そして、アクセス制御装置10は、アクセス許可破棄命令を生成し、リソース提供装置20へ送信する(ステップS108)。リソース提供装置20は、アクセス許可破棄命令を受信すると、アクセス管理テーブル204を参照し、リソース利用装置30に関する情報を削除する(ステップS109)。その後、アクセス管理テーブル204から情報が削除されたリソース利用装置30からアクセス命令が送信されてきても、送信されたアクセス命令に記録されたコマンド及び装置IDは、アクセス管理テーブル204に記録されていないため、リソース提供装置20はアクセス命令を受け付けなくなる。したがって、リソース提供装置20は、アクセス管理テーブル204に情報が記録されていないリソース利用装置30からのアクセスを拒否するため、リソース利用装置30は、リソースを利用することができなくなる。

[0087] また、アクセス制御装置10は、リソース提供装置20に通知した装置IDを有するリソース利用装置30に関する情報を許可情報管理テーブル104から削除する(ステップS110)。

[0088] 図9は、リソース提供装置20によるリソースアクセス制御の流れの一例を示すシーケンス図である。

[0089] リソース提供装置20は、アクセス制御装置10からアクセス許可命令を受信すると(ステップS201)、所定の処理を行った後、完了通知を送信する。その後、アクセス制御装置10からリソース利用装置30へアクセス許可通知命令が送信される(ステップS203)。

[0090] リソース提供装置20は、一定時間毎にアクセス制御装置10の存在を確認する(ステップS204)。アクセス制御装置10の存在が確認できた場合(ステップS205)、リソ

ース提供装置20は、リソース利用装置30からアクセス命令が送信されてくると(ステップS206)、リソース利用装置30からのアクセスを許可する(ステップS207)。

[0091] 一方、アクセス制御装置10の存在が確認できなかった場合(ステップS208)、リソース提供装置20は、アクセス制御装置10に関する情報アクセス管理テーブル204から削除する(ステップS209)。これにより、アクセス管理テーブル204から情報が削除されたリソースリ利用装置30からアクセスの要求があった場合(ステップS210)、リソース提供装置20は、アクセスを拒否する(ステップS211)。

[0092] なお、リソース利用装置30からのアクセスを拒否した場合、リソース提供装置20がリソース利用装置30に対してアクセスが失敗した理由を示すエラーコードを送信することとしてもよい。

[0093] 図10は、アクセス制御装置10におけるアクセス許可部106、存在確認部107及びアクセス破棄部108の動作を示すフローチャートである。

[0094] まず、アクセス制御装置10において、アクセス許可部106は、アクセス制御に必要な情報を許可情報管理テーブル104に記録する。許可情報管理テーブル104に記録される情報は、例えば、リソース提供装置20に関する情報(図2に示す提供側11に相当)、リソース利用装置30に関する情報(図2に示す利用側12に相当)、アクセス制御装置10及びリソース利用装置30の間の通信I/F(図2に示す通信I/F13に相当)、リソース提供装置20がリソース利用装置30に対してどのようなアクセスを可能とするかに関する情報(図2に示すアクセス14に相当する情報であって、リソース提供装置20がリソース利用装置30から受け付け可能な命令(書き込み命令、読み込み命令、所望の実行命令等)、及び命令が及ぶ範囲(ディレクトリの情報などのパラメータ制限に関する情報))である。

[0095] そして、アクセス許可部106は、アクセス許可命令を生成して通信部101に渡す。アクセス許可命令は、通信部101を介してリソース提供装置20へ送信される(ステップS11)。

[0096] アクセス許可部106は、通信部101から完了通知を受け取ると(ステップS12)、アクセス許可通知命令を生成して通信部101に渡す。アクセス許可通知命令は、通信部101を介してリソース利用装置30へ送信される(ステップS13)。

[0097] 次に、存在確認部107は、リソース利用装置30の存在を確認する(ステップS14)。存在確認部107は、存在確認命令を生成して通信部101に渡す。そして、存在確認部107は、リソース利用装置30の存在が確認できたか否かを判断する(ステップS15)。存在確認部107は、通信部101から応答を受け取ったか否かを判断する。通信部101は、リソース利用装置30から送信されてきた応答を存在確認部107に渡す。

[0098] ステップS15において、リソース利用装置30の存在が確認できた場合、つまり、通信部101から応答を受け取った場合、存在確認部107は、一定時間スリープする(ステップS14)。そして、存在確認部107は、一定時間スリープした後、再びリソース利用装置30の存在を確認する。

[0099] 一方、ステップS15において、リソース利用装置30の存在が確認できなかった場合、つまり、通信部101から応答を受け取っていない場合、存在確認部107は、応答を受け取ることができなかったリソース利用装置30の装置IDをアクセス破棄部108に通知する。

[0100] アクセス破棄部108は、通知された装置IDを記録したアクセス許可破棄命令を生成し、通信部101に渡す。アクセス許可破棄命令は、通信部101を介してリソース提供装置20に送信される(ステップS17)。

[0101] そして、アクセス破棄部108は、許可情報管理テーブル104を参照し、通知された装置IDを有するリソース利用装置30に関する情報を削除する(ステップS18)。

[0102] 次に、図2に示す許可情報管理テーブル104を用いた場合における、アクセス制御装置10による存在確認命令及びアクセス許可破棄命令送信の具体例について説明する。

[0103] アクセス制御装置10は、許可情報管理テーブル104に記録されている順番に従い、利用側12に記録されている装置IDを有するリソース利用装置30の存在を確認する。また、アクセス制御装置10は、許可情報管理テーブル104に記録されているリソース利用装置30の存在を確認する際、リソース利用装置30の装置IDに対応付けられている通信インターフェース102を用いて通信する。

[0104] 例えば、図2の1行目に記録されている管理情報を例に説明すると、アクセス制御装置10は、通信インターフェースeth0を利用して携帯電話Eと通信し、携帯電話E

の存在を確認する。そして携帯電話Eの存在が確認できなかった場合、アクセス制御装置10は、リソース提供装置20である携帯電話Bに対してアクセス許可破棄命令を送信し、携帯電話Eによる秘密資料参照のアクセスを拒否するよう命令する。また、アクセス制御装置10は、利用側12に記録されている携帯電話Eに関する情報(提供側11、通信I／F13及びアクセス14)を削除する。

[0105] また、図2の2行目に記録されている管理情報を例に説明すると、アクセス制御装置10は、すべての通信インターフェースを利用して携帯電話Bと通信し、携帯電話Bの存在を確認する。そして、どの通信インターフェースで通信しても携帯電話Bの存在が確認できなかった場合、アクセス制御装置10は、リソース提供装置20である据置機器Cに対してアクセス許可破棄命令を送信し、携帯電話Bによるビデオ視聴のアクセスを拒否するよう命令する。また、アクセス制御装置10は、利用側12に記録されている携帯電話Bに関する情報(提供側11、通信I／F13及びアクセス14)を削除する。

[0106] 図11は、アクセス制御装置10における存在確認応答部105の動作を示すフローチャートである。

[0107] まず、存在確認応答部105は、通信部101を介してリソース提供装置20から送信されてきた存在確認命令を受け取ったか否かを判断する(ステップS21)。存在確認命令を受け取っていない場合、存在確認応答部105は処理を終了する。

[0108] 一方、存在確認命令を受け取った場合、存在確認応答部105は、存在確認命令に対する応答を生成して、通信部101に渡す。応答は、通信部101を介して存在確認命令の送信元であるリソース提供装置20へ送信される(ステップS22)。

[0109] 図12は、リソース提供装置20の動作を示すフローチャートである。

[0110] まず、リソース提供装置20において、リソースアクセス許可部205は、通信部201を介してアクセス制御装置10から送信されてきたアクセス許可命令を受信すると(ステップS31)、アクセス管理テーブル204を更新する。具体的には、リソースアクセス許可部205は、アクセス管理テーブル204を参照し、アクセス許可命令に記録されているリソース利用装置30に対応する装置IDを制御側21に記録し、制御情報をアクセス201に記録する。

[0111] そして、リソースアクセス許可部205は、リソース利用装置30との通信が可能となるように設定を行い、設定が完了すると、完了通知を生成して通信部201に渡す。完了通知は、通信部201を介してアクセス制御装置10へ送信される(ステップS32)。

[0112] 次に、存在確認部206は、アクセス制御装置10の存在を確認する(ステップS33)。具体的には、存在確認部206は、存在確認命令を生成して通信部201に渡す。そして、存在確認部206は、アクセス制御装置10の存在が確認できたか否かを判断する(ステップS34)。具体的には、存在確認部206は、通信部201から応答を受け取ったか否かを判断する。通信部201は、アクセス制御装置10から送信されてきた応答を存在確認部107に渡す。

[0113] ステップS34において、アクセス制御装置10の存在が確認できた場合、つまり、通信部201から応答を受け取った場合、存在確認部206は、一定時間スリープする(ステップS35)。そして、存在確認部206は、一定時間スリープした後、再びアクセス制御装置10の存在を確認する。

[0114] 一方、ステップS34において、アクセス制御装置10の存在が確認できなかった場合、つまり、通信部201から応答を受け取っていない場合、存在確認部206は、応答を受け取ることができなかったアクセス制御装置10の装置IDをアクセス破棄部207に通知する。

[0115] アクセス破棄部207は、アクセス管理テーブル204を参照し、通知された装置IDを有するアクセス制御装置10に関する情報を全て削除する(ステップS36)。これにより、アクセス制御装置10に対応付けて記録されているリソース利用装置30に関する情報が削除されるため、その後、リソース提供装置20は、アクセス管理テーブル204から削除されたリソース利用装置30からのアクセスを拒否する。

[0116] 次に、図3に示すアクセス管理テーブル204を用いた場合における、リソース提供装置20による存在確認の具体例について説明する。

[0117] リソース提供装置20は、アクセス管理テーブル204に記録されている順番に従い、制御側21に記録されている装置IDを有するアクセス制御装置10の存在を確認する。

[0118] 例えば、図3の2行目に記録されている管理情報を例に説明すると、リソース提供装

置20は、制御側21に記録されている携帯電話Hの存在を確認する。そして携帯電話Hの存在が確認できなかった場合、制御側21に記録されている携帯電話Hに関する情報(制御側21、利用側22及びアクセス23)を削除する。この場合、利用側22から携帯電話B及び携帯電話Eの装置IDが削除される。これにより、携帯電話Bは、リソース提供装置20にアクセスしてビデオ視聴することができなくなり、また携帯電話Eは、リソース提供装置20にアクセスして資料を印刷することができなくなる。

[0119] 図13は、リソース提供装置20におけるアクセス破棄部207の動作を示すフローチャートである。まず、アクセス破棄部207は、通信部201からアクセス許可破棄命令を受け取ったか否かを判断する(ステップS41)。アクセス許可破棄命令を受け取っていない場合、処理を終了し、一方、アクセス許可破棄命令を受け取った場合、アクセス管理テーブル204を参照し、アクセス許可破棄命令に記録されている装置IDを有するアクセス制御装置10に関する情報を全て削除する(ステップS42)。

[0120] 図14は、リソース利用装置30の動作を示すフローチャートである。まず、リソース利用装置30において、存在確認応答部302は、通信部301を介してアクセス制御装置10から送信されてきた存在確認命令を受け取ったか否かを判断する(ステップS51)。存在確認命令を受け取っていない場合、存在確認応答部302は処理を終了する。

[0121] 一方、存在確認命令を受け取った場合、存在確認応答部302は、応答を生成して、通信部301に渡す。応答は、通信部301を介して存在確認命令の送信元であるアクセス制御装置10へ送信される(ステップS52)。

[0122] 以上のように、本実施の形態によれば、アクセス制御装置は、存在が確認できないリソース利用装置からのアクセスを拒否するようリソース提供装置に命令する。リソース提供装置は、アクセス制御装置からの命令に従い、管理テーブルからリソース利用装置に関する情報を削除することで、その後のリソース利用装置からのアクセスを拒否する。これにより、不要なアクセス許可を速やかに破棄し、リソース利用装置を利用したリソース提供装置への不正なアクセスを防止することができる。したがって、システムの秘匿性を向上させることができる。

[0123] また、リソース提供装置とアクセス制御装置との間の通信が途絶えた場合、アクセス

制御装置がリソース提供装置に対して、アクセス許可破棄命令を送信することができなくなる。その場合、セキュリティの観点から、リソース提供装置が自装置にアクセスするアクセス利用装置に対するアクセス制御を破棄することが望ましい。

[0124] この場合においても、本実施の形態によれば、リソース提供装置は、アクセス制御装置の存在が確認できなくなると、存在が確認できなくなったアクセス制御装置及びアクセス制御装置によりアクセス制御されているリソース利用装置に関する情報をアクセス管理テーブルから削除する。その後、リソース提供装置はアクセス管理テーブルから情報が削除されたリソース利用装置からのアクセスを拒否する。これにより、アクセス制御装置からアクセス許可破棄命令を送信することができない場合であっても、不要なアクセス許可を速やかに破棄し、リソース利用装置を利用したリソース提供装置への不正なアクセスを防止することができる。したがって、さらにシステムの秘匿性を向上させることができる。

[0125] なお、本実施の形態では、アクセス制御装置がリソース利用装置へアクセス許可通知命令を送信していた。ここで、実装によっては、アクセス制御装置ではなく、リソース提供装置がアクセス許可通知命令を生成し、リソース利用装置へ送信することとしてもよい。また、ユーザがリソース提供装置にアクセスするために必要な情報を直接リソース利用装置に入力してもよい。重要なのは、リソース利用装置にリソース利用が許可されたことを通知することである。

[0126] また、本実施の形態では、アクセス制御装置及びリソース提供装置は、許可情報管理テーブルまたはアクセス管理テーブルを用いて複数の電子機器に関する情報を管理していた。ここで、管理対象の電子機器が1台のみである場合には、許可情報管理テーブルまたはアクセス管理テーブルを備えていなくてもよい。

[0127] また、本実施の形態では、アクセス許可命令、アクセス許可通知命令、及びアクセス許可破棄命令には、制御情報が記録されるものとして説明した。ここで、実施によっては、これらの命令に制御情報を添付しなくてもよい。例えば、制御されるコマンドやパラメータが、システム設計時にあらかじめ決定されている場合には、命令に制御情報を添付する必要はない。また、図3に示すデータ構造体は一例であり、上述の3つの命令のそれぞれが上記構造体に従わなくてもよい。例えば、アクセス制御装置と

リソース提供装置との間で予め決められた整理番号を利用し、アクセス許可破棄命令の中身はその整理番号だけで決められるようにしてもよい。その場合、整理番号が記録されたアクセス許可破棄命令を受信したリソース提供装置は、受信した整理番号に基づいてどのアクセス許可を破棄すべきかを決定する。

[0128] また、本実施の形態では、アクセス制御装置によるリソース利用装置の監視と、リソース提供装置によるアクセス制御装置の監視とを並行して実施していた。ここで、アクセス制御装置による監視及びリソース提供装置による監視を並行して実施する必要がない場合には、アクセス制御装置またはリソース提供装置のいずれかの監視のみを実施することとしてもよい。

[0129] また、本実施の形態では、アクセス制御装置は、許可情報管理テーブルに記録されている全てのリソース利用装置の存在を確認していた。ここで、アクセス制御装置は、許可情報管理テーブルに記録されているリソース提供装置のうち、アクセス許可の破棄制御が必要なリソース提供装置に対応付けて記録されているリソース利用装置の存在を確認することとしてもよい。これにより、許可情報管理テーブルに記録されているリソース提供装置の全てについてアクセス許可の破棄制御を実施する必要がない場合に、効率よくアクセス制御処理を行うことができる。

[0130] また、本実施の形態では、アクセス制御装置とリソース提供装置とが相互に通信するために必要な設定が既に確立されているものとして説明した。ここで、アクセス制御装置及びリソース提供装置が通信を確立するための設定が必要な場合、リソース提供装置が保持するアクセス管理テーブルに通信I／Fに関する情報を記録することとしてもよい。

[0131] なお、UPnPの技術を用いれば、通信路に接続された装置同士は、通信する際に互いのIPアドレスを得ることができる。したがって、命令に含まれる装置IDがIPアドレスそのものである場合、命令を受け取った電子機器は、通信相手先を特定することができる。また、装置IDが、MACアドレスや公開鍵、ハッシュ値等のIPアドレス以外の情報である場合、電子機器は、装置IDとIPアドレスとを対応付けて保持するサーバ(図示せず)へ装置IDを通知し、IPアドレスの検索を依頼することとしてもよい。または、装置IDに対応するIPアドレスを検索した電子機器が、通信路に接続されている全

ての電子機器に対して装置IDをブロードキャスト送信し、検索対象の装置IDを有する装置が自身のIPアドレスを返信することにより、IPアドレスを得ることとしてもよい。

[0132] 以下、実施の形態1において説明したアクセス制御システムの動作の具体例について説明するが、本発明はかかる実施例のみに限定されるものではない。

[0133] （実施例1）

実施例1では、アクセス制御処理の具体例について説明する。ここで、A社内にあるサーバがリソース提供装置、A社の甲氏が所有する携帯電話がアクセス制御装置、B社内にあるパーソナルコンピュータがリソース利用装置に相当する場合を例に説明する。また、サーバと携帯電話との間は、携帯電話網およびインターネットを介したIP接続で接続され、サーバとパーソナルコンピュータとの間は、インターネットを介したIP接続で接続され、携帯電話とパーソナルコンピュータとの間は、短距離無線を介したIP接続で接続されているものとする。

[0134] サーバには、甲氏の重要なデータが格納されている。甲氏は、B社の乙氏を訪問した際、A社内のサーバが保持する情報を、B社内のパーソナルコンピュータを通じて一時的に表示する必要がある。このとき、A社の甲氏は、携帯電話を操作することにより、パーソナルコンピュータからサーバへのアクセスを許可する。これにより、B社内のパーソナルコンピュータから、A社内のサーバが保持するデータにアクセスすることができる。

[0135] B社内のパーソナルコンピュータからサーバ内のデータにアクセスしている間、携帯電話は、短距離無線を利用してパーソナルコンピュータの存在を一定時間毎に確認する。甲氏が乙氏への訪問を終え、B社から離れると、パーソナルコンピュータと携帯電話との距離が大きくなっていく。携帯電話は、短距離無線の接続が切断された時点で、アクセス管理テーブル204からパーソナルコンピュータに関する情報を削除するようサーバに命令する。これにより、A氏がB社を離れた後、パーソナルコンピュータからサーバへのアクセス許可を速やかに破棄することができる。したがって、パーソナルコンピュータを用いたサーバへの不正なアクセスを防止することができるため、システムの秘匿性を向上させることができる。

[0136] また、アクセス制御装置とリソース利用装置との間を無線で接続し、無線による通信

が可能な範囲を所定の範囲に制限することとすれば、アクセス制御装置がリソース利用装置の存在を確認する際に、リソース利用装置がネットワーク上に存在するか否かと、リソース利用装置が存在する位置が所定の範囲内であるか否かとを同時に確認することができる。

[0137] なお、本実施例では、アクセス制御装置である携帯電話がリソース利用装置であるパーソナルコンピュータの存在を確認していればよく、リソース提供装置であるサーバは、携帯電話の存在を確認しなくとも、アクセスを破棄すべきリソース利用装置(パーソナルコンピュータ)からのアクセスを速やかに破棄することが可能となる。

[0138] (実施例2)

次に、アクセス制御処理及びリソースアクセス制御処理の具体例について説明する。ここで、A社内にあるサーバがリソース提供装置、A社の甲氏が所有する携帯電話がアクセス制御装置、B社の乙氏が所有する携帯端末がリソース利用装置に相当する場合を例に説明する。本実施例において、携帯電話とサーバとの間、及び携帯電話と携帯端末との間は、それぞれ短距離無線を介したIP接続で接続されており、サーバと携帯端末との間は、インターネットを介したIP接続で接続されているものとする。また、サーバは短距離無線を利用して携帯電話の存在を確認し、その通信範囲は、1つの部屋をカバーする程度の大きさであるものとする。

[0139] B社の乙氏がA社の甲氏を訪問した際、甲氏は、携帯電話を操作することにより、乙氏が所有する携帯端末からサーバへのアクセスを許可する。サーバは、一定時間毎に甲氏が所有する携帯電話が自装置の通信範囲内に存在するか否かを確認する。例えば、甲氏が部屋から離れ、サーバが甲氏が所有する携帯電話の存在を確認することができなくなると、アクセス管理テーブル204から携帯電話に関する情報を削除する。このとき、乙氏が所有する携帯端末に関する情報もアクセス管理テーブル204から削除されるため、サーバは、携帯端末からのアクセスを拒否する。これにより、携帯端末を利用してサーバに不正にアクセスすることを防止することができる。

[0140] また、乙氏が訪問を終えてA社から離れると、甲氏が所有する携帯電話は、乙氏が所有する携帯端末の存在を確認することができなくなるため、携帯端末に関する情報を削除するようサーバに命令する。また、それと共に、携帯電話は、自身が保持す

る許可情報管理テーブル104から携帯端末に関する情報を削除する。

[0141] 以上のように、本実施例によれば、アクセス制御装置は、リソース利用装置が通信範囲内に存在するか否かを監視し、リソース提供装置は、アクセス制御装置が通信範囲内に存在するか否かを監視する。このように、通信範囲を近距離に限定してリソース利用装置またはアクセス制御装置の存在を確認することにより、リソース利用装置30、及びアクセス制御装置10が所定の範囲内に位置する場合にのみ、リソース提供装置20を利用することができるようにすることができる。

産業上の利用可能性

[0142] 本発明は、電子機器のアクセス制御に関して、リソース利用装置からのアクセスを速やかに破棄し、リソース提供装置の不正な使用を防止するアクセス制御装置、アクセス制御装置からの要求に応じてリソース利用装置からのアクセスを受け付けるリソース提供装置、及びこれらを用いたアクセス制御システム等として有用である。

請求の範囲

[1] リソース提供装置で提供されるリソースを利用するために行われるリソース利用装置からリソース提供装置へのアクセスを制御するアクセス制御装置であって、

前記リソース利用装置及び前記リソース提供装置と通信する通信部と、

前記リソース利用装置からのアクセスを許可するよう、前記通信部を介して前記リソース提供装置へ命令するアクセス許可部と、

前記アクセス許可部によってアクセスが許可された前記リソース利用装置に関する情報を管理情報として格納する記憶部と、

前記記憶部に前記管理情報が格納されているリソース利用装置との通信状態を前記通信部を介して確認する存在確認部と、

前記存在確認部によって通信が途絶えたと判断されたリソース利用装置からのアクセスを拒否するよう、前記通信部を介して前記リソース提供装置へ命令するアクセス破棄部とを備える、アクセス制御装置。

[2] 前記アクセス破棄部は、前記通信が途絶えたと判断されたリソース利用装置に関する情報を前記記憶部から削除する、請求項1に記載のアクセス制御装置。

[3] 前記リソース利用装置に関する情報は、前記リソース利用装置を識別するための情報である、請求項1に記載のアクセス制御装置。

[4] 前記リソース利用装置に関する情報は、前記リソース利用装置を識別するための情報と、当該リソース利用装置からのアクセスを受け付けるリソース提供装置を識別するための情報とを含む、請求項1に記載のアクセス制御装置。

[5] 前記リソース利用装置に関する情報は、前記リソース利用装置が前記リソース提供装置へアクセスする際に発行するコマンドに関する情報を含む、請求項3または4に記載のアクセス制御装置。

[6] 前記アクセス許可部は、アクセスを許可すべきリソース利用装置に関する情報を、前記通信部を介して前記リソース提供装置へ通知する、請求項1に記載のアクセス制御装置。

[7] 前記アクセス破棄部は、前記通信が途絶えたと判断されたリソース利用装置に関する情報を、前記通信部を介して前記リソース提供装置へ通知する、請求項1に記載

のアクセス制御装置。

[8] さらに、前記通信部を介して前記リソース提供装置から通信状態の確認要求を受け取ると、当該通信部を介して当該リソース提供装置へ応答する生存確認応答部を備える、請求項1に記載のアクセス制御装置。

[9] 前記通信部は、前記リソース利用装置と無線を介して通信し、

前記無線による通信範囲は所定の範囲に制限されている、請求項1に記載のアクセス制御装置。

[10] アクセス制御装置よりアクセスが許可されたリソース利用装置からのアクセスを受け付け、リソースを提供するリソース提供装置であって、

前記アクセス制御装置及び前記リソース利用装置と通信する通信部と、

前記通信部を介して前記アクセス制御装置から命令されたリソース利用装置に関する情報を管理情報として格納する記憶部と、

前記記憶部に前記管理情報が格納されているリソース利用装置からのアクセスを許可するアクセス許可部と、

前記アクセス制御装置との通信状態を前記通信部を介して確認する存在確認部と、

前記存在確認部によって通信が途絶えたと判断されたアクセス制御装置によってアクセスが許可されたリソース利用装置からのアクセスを拒否するアクセス拒否部とを備える、リソース提供装置。

[11] 前記アクセス拒否部は、前記通信が途絶えたと判断されたアクセス制御装置によってアクセスが許可されたリソース利用装置に関する情報を前記記憶部から削除する、請求項10に記載のリソース提供装置。

[12] 前記リソース利用装置に関する情報は、前記リソース利用装置を識別するための情報である、請求項10に記載のリソース提供装置。

[13] 前記リソース利用装置に関する情報は、前記リソース利用装置を識別するための情報と、当該リソース利用装置に対してアクセスを許可したアクセス制御装置を識別するための情報とを含む、請求項10に記載のリソース提供装置。

[14] 前記リソース利用装置に関する情報は、前記リソース利用装置が前記リソース提供

装置へアクセスする際に発行するコマンドに関する情報を含む、請求項12または13に記載のリソース提供装置。

[15] 前記アクセス拒否部は、前記リソース利用装置からのアクセスを拒否するよう、前記通信部を介して前記アクセス制御部から命令されると、命令されたリソース利用装置からのアクセスを拒否する、請求項10に記載のリソース提供装置。

[16] 前記アクセス拒否部は、前記命令されたリソース利用装置に関する情報を前記記憶部から削除する、請求項15に記載のリソース提供装置。

[17] 前記通信部は、前記アクセス制御装置と無線を介して通信し、

前記無線による通信範囲は所定の範囲に制限されている、請求項10に記載のリソース提供装置。

[18] リソースを提供するリソース提供装置と、当該リソースへアクセスするリソース利用装置と、当該リソース利用装置によるアクセスを制御するアクセス制御装置とを備えるアクセス制御システムであって、

前記アクセス制御装置は、

前記リソース利用装置及び前記リソース提供装置と通信する通信部と、

前記リソース利用装置からのアクセスを許可するよう、前記通信部を介して前記リソース提供装置へ命令するアクセス許可部と、

前記アクセス許可部によってアクセスが許可された前記リソース利用装置に関する情報を管理情報として格納する記憶部と、

前記記憶部に前記管理情報が格納されているリソース利用装置との通信状態を前記通信部を介して確認する存在確認部と、

前記存在確認部によって通信が途絶えたと判断されたリソース利用装置からのアクセスを拒否するよう、前記通信部を介して前記リソース提供装置へ命令するアクセス破棄部とを含み、

前記リソース提供装置は、

前記アクセス制御装置及び前記リソース利用装置と通信するリソース提供通信部と、

前記リソース提供通信部を介して前記アクセス制御装置から命令されたリソース

利用装置に関する情報を管理情報として格納するリソース提供記憶部と、

前記リソース提供記憶部に前記管理情報が格納されているリソース利用装置からのアクセスを許可するリソースアクセス許可部と、

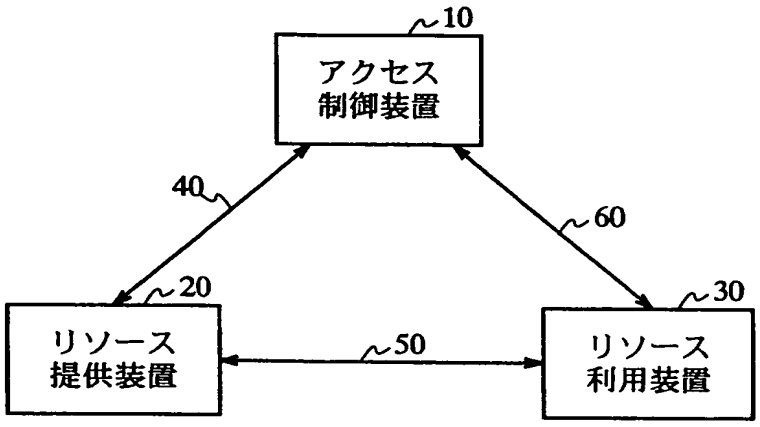
前記アクセス制御装置との通信状態を前記リソース提供通信部を介して確認するリソース提供存在確認部と、

前記リソース提供存在確認部によって通信が途絶えたと判断されたアクセス制御装置によってアクセスが許可されたリソース利用装置、及び前記リソース提供通信部を介して前記アクセス制御装置から命令されたリソース利用装置からのアクセスを拒否するアクセス拒否部とを含む、アクセス制御システム。

要 約 書

破棄すべきアクセス許可を速やかに破棄し、リソースを提供する機器の不正な使用を防止することを目的とする。アクセス制御装置10において、通信部101は、リソース利用装置30及びリソース提供装置20と通信する。アクセス許可部106は、リソース利用装置30からのアクセスを許可するよう、通信部101を介して前記リソース提供装置20へ命令する。記憶部103は、アクセス許可部106によってアクセスが許可された前記リソース利用装置に関する情報を管理情報として格納する。存在確認部107は、記憶部103に前記管理情報が格納されているリソース利用装置30との通信状態を通信部101を介して確認する。アクセス破棄部108は、存在確認部107によって通信が途絶えたと判断されたリソース利用装置30からのアクセスを拒否するよう、通信部101を介してリソース提供装置20へ命令する。

[図1]



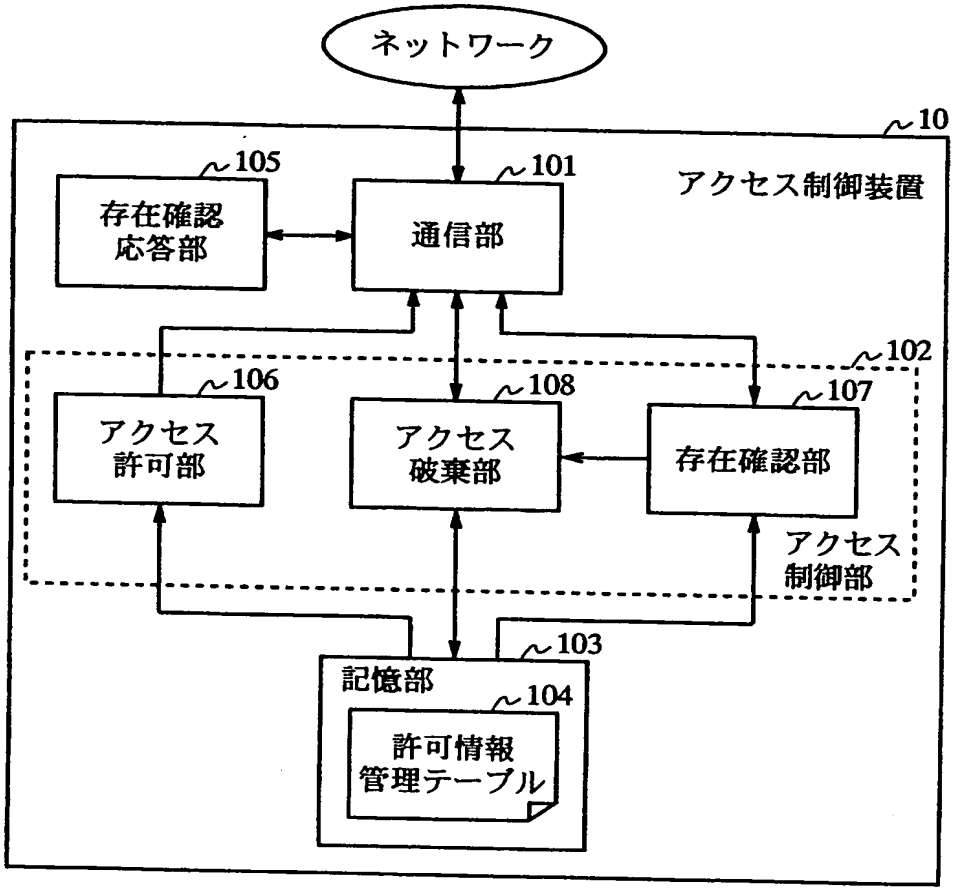
[図2]

11	12	13	14	
提供側	利用側	通信I/F	アクセス	104
携帯電話B	携帯電話E	eth0	秘密資料参照	
据置機器C	携帯電話B	ANY	ビデオ視聴	
パソコンD	携帯電話E	eth1	印刷	
据置機器C	携帯電話F	ttyS0	リモコン制御	
パソコンD	パソコンG	eth0	ファイル書き込み	

[図3]

21	22	23	
制御側	利用側	アクセス	204
携帯電話B	携帯電話E	秘密資料参照	
携帯電話H	携帯電話B	ビデオ視聴	
携帯電話H	携帯電話E	印刷	
据置機器I	据置機器F	リモコン制御	
パソコンJ	パソコンG	ファイル書き込み	

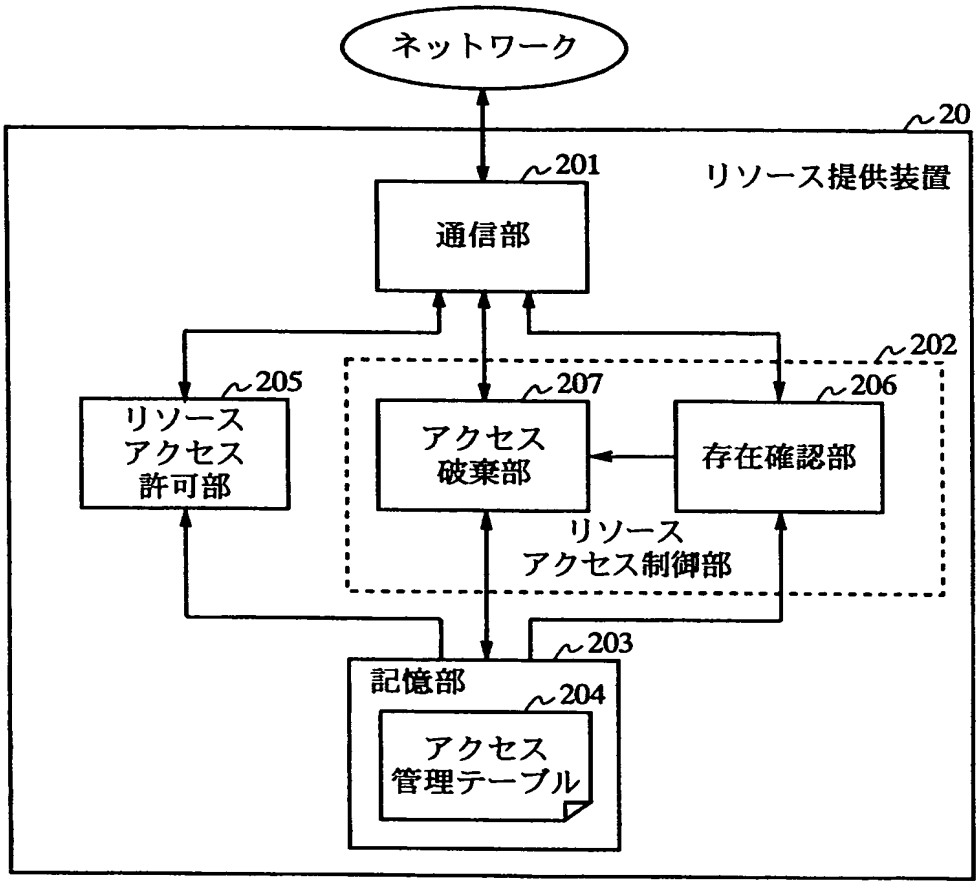
[図4]



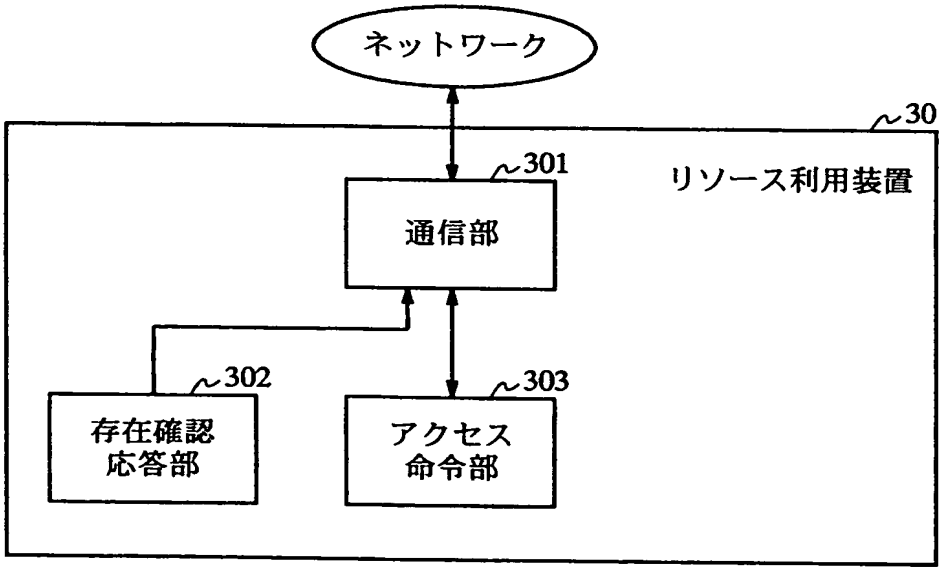
[図5]

タイプ	
装置ID	
制御情報	コマンド
	パラメータ制限

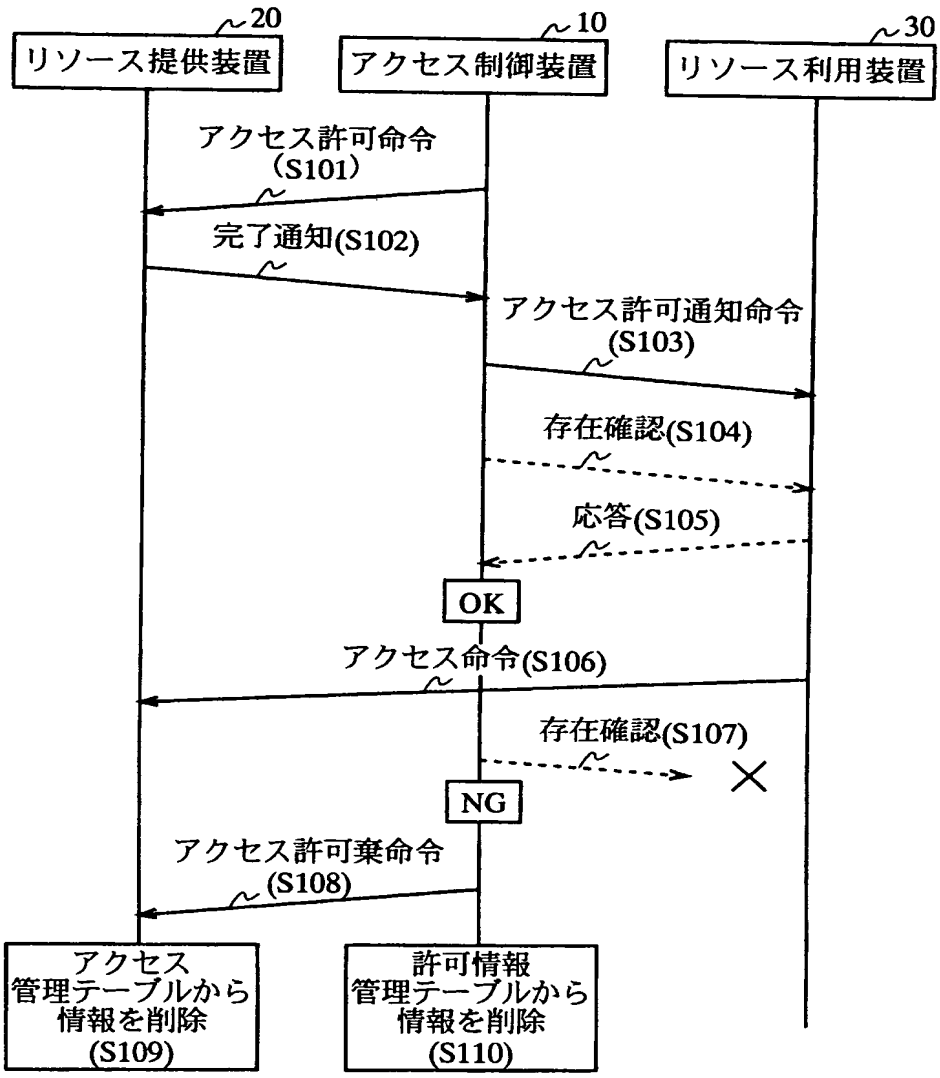
[図6]


ネットワーク
20
リソース提供装置
201
通信部
202
205
リソース
アクセス
許可部
207
アクセス
破棄部
206
存在確認部
リソース
アクセス制御部
203
記憶部
204
アクセス
管理テーブル

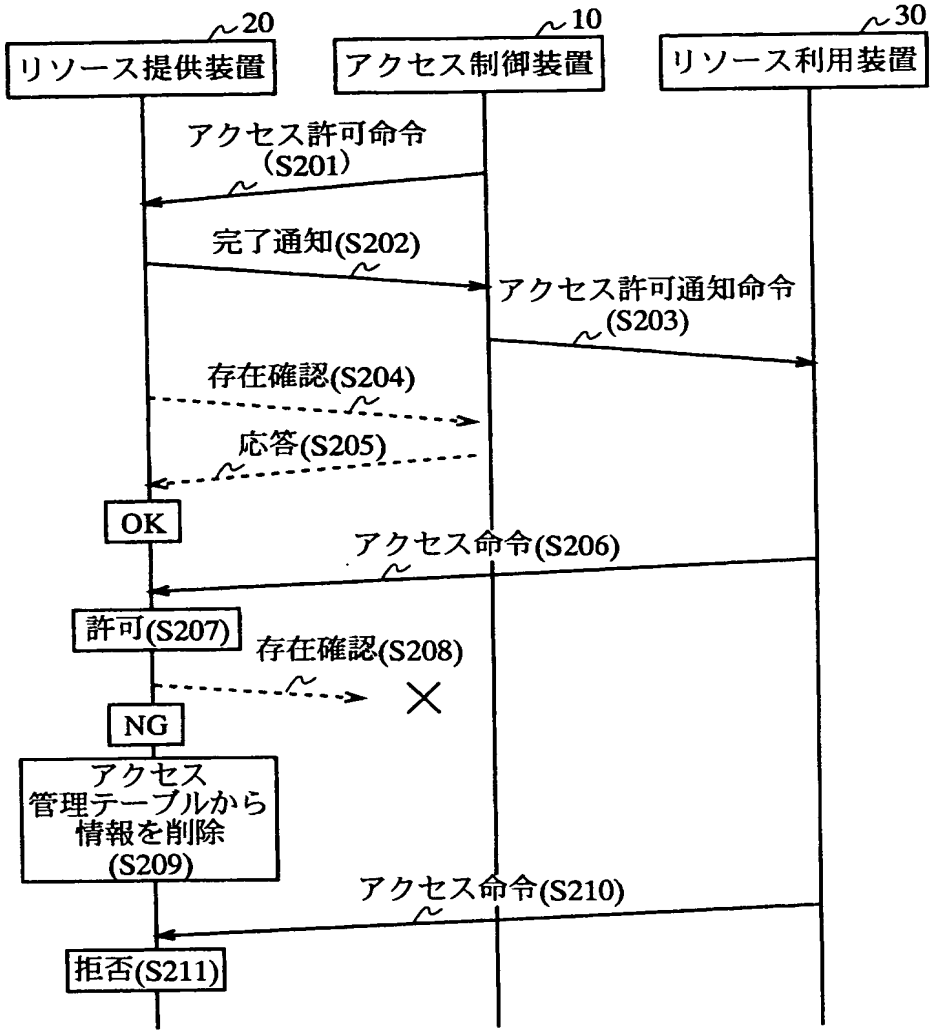
[図7]


ネットワーク
30
リソース利用装置
301
通信部
302
存在確認
応答部
303
アクセス
命令部

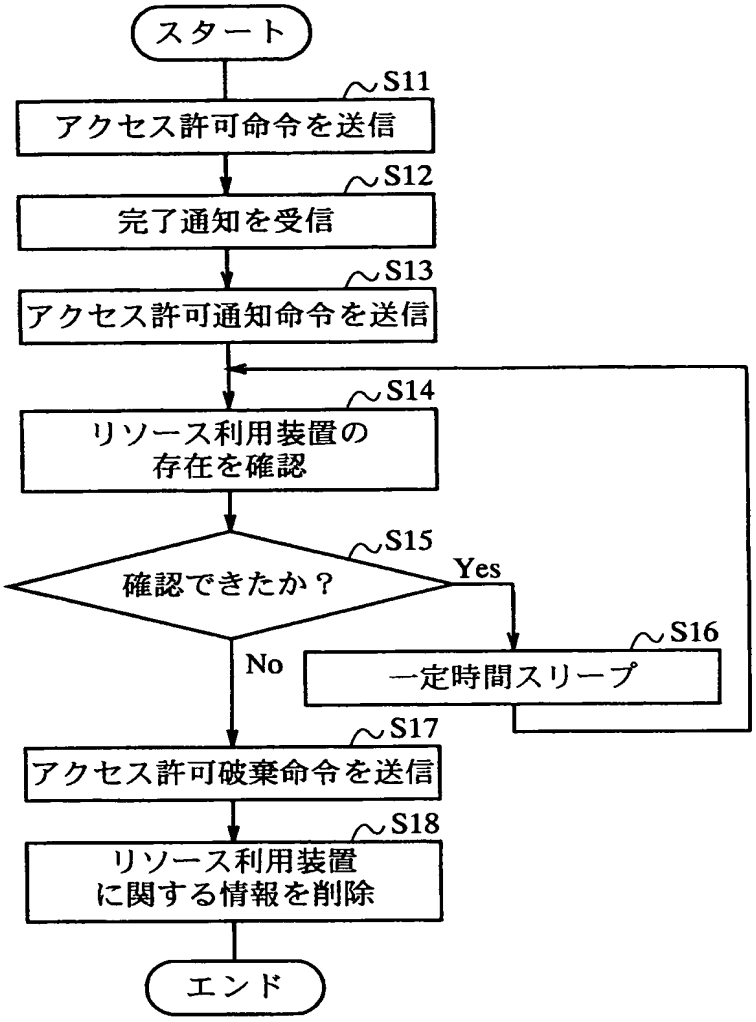
[図8]


20
リソース提供装置
10
アクセス制御装置
30
リソース利用装置
アクセス許可命令
(S101)
完了通知(S102)
アクセス許可通知命令
(S103)
存在確認(S104)
応答(S105)
OK
アクセス命令(S106)
存在確認(S107)
NG
アクセス許可棄命令
(S108)
アクセス
管理テーブルから
情報を削除
(S109)
許可情報
管理テーブルから
情報を削除
(S110)

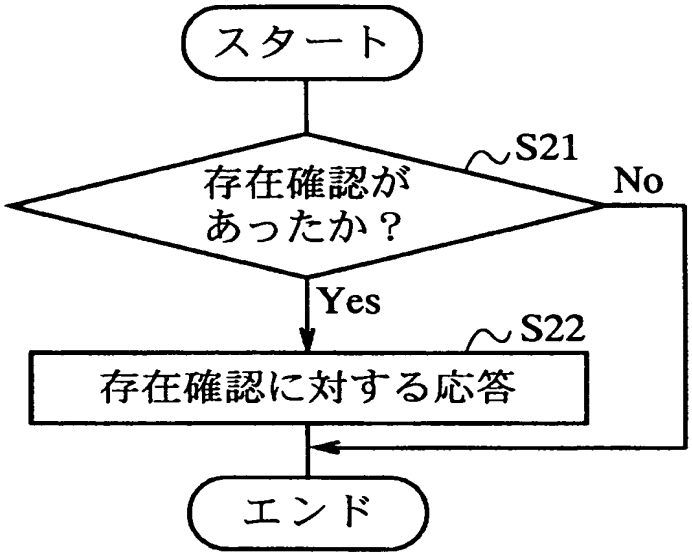
[図9]


20
リソース提供装置
10
アクセス制御装置
30
リソース利用装置
アクセス許可命令
(S201)
完了通知(S202)
アクセス許可通知命令
(S203)
存在確認(S204)
応答(S205)
OK
アクセス命令(S206)
許可(S207)
存在確認(S208)
NG
アクセス
管理テーブルから
情報を削除
(S209)
アクセス命令(S210)
拒否(S211)

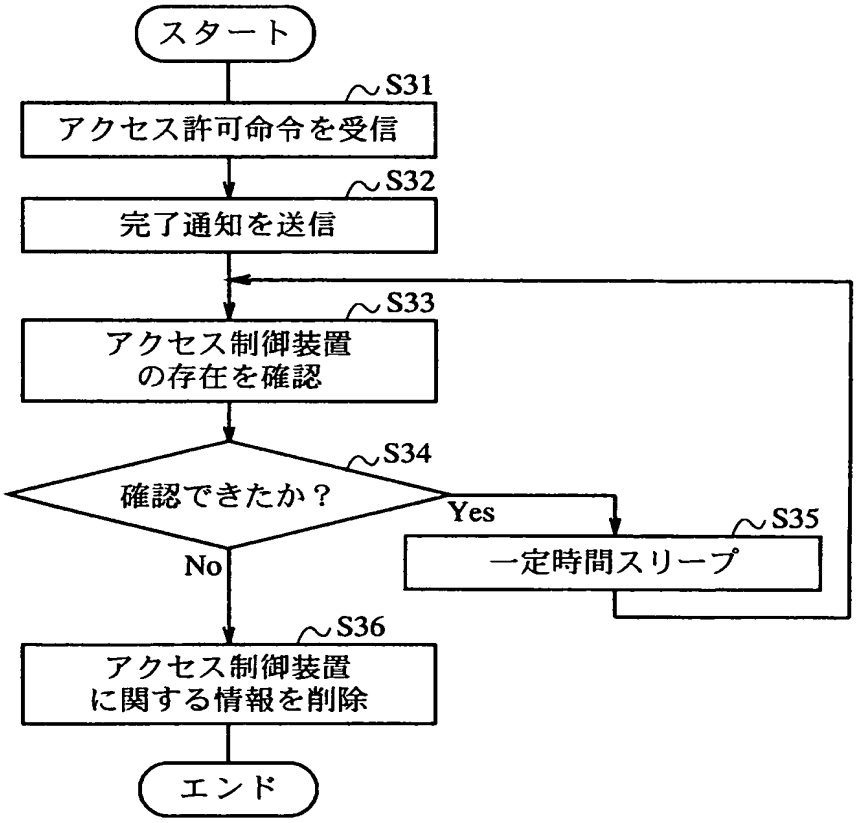
[図10]


スタート
S11
アクセス許可命令を送信
S12
完了通知を受信
S13
アクセス許可通知命令を送信
S14
リソース利用装置の
存在を確認
S15
確認できたか？
Yes
No
S16
一定時間スリープ
S17
アクセス許可破棄命令を送信
S18
リソース利用装置
に関する情報を削除
エンド

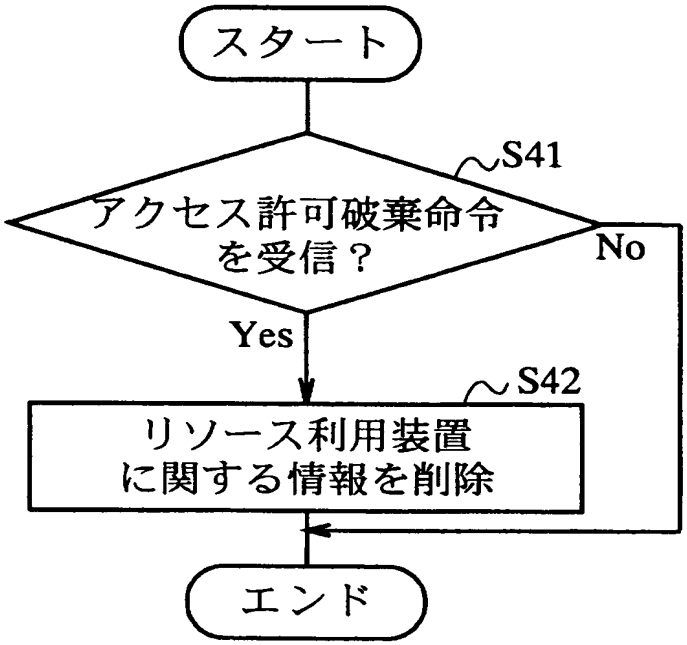
[図11]


スタート
S21
存在確認が
あったか？
No
Yes
S22
存在確認に対する応答
エンド

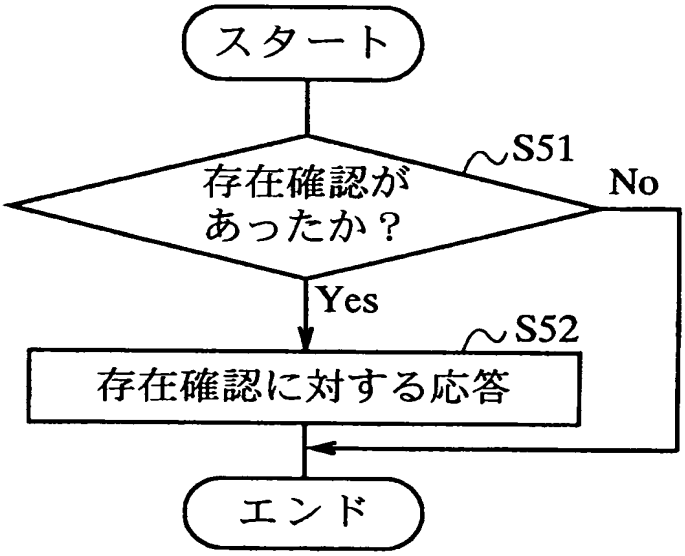
[図12]


スタート
S31
アクセス許可命令を受信
S32
完了通知を送信
S33
アクセス制御装置
の存在を確認
S34
確認できたか？
Yes
S35
一定時間スリープ
No
S36
アクセス制御装置
に関する情報を削除
エンド

[図13]


スタート
S41
アクセス許可破棄命令
を受信？
No
Yes
S42
リソース利用装置
に関する情報を削除
エンド

[図14]


スタート
S51
存在確認が
あったか？
No
Yes
S52
存在確認に対する応答
エンド